STRUCTURE OF THE REDUCED RESIDUE SYSTEM WITH COMPOSITE MODULUS

HUGO S. SUN
California State University, Fresno, California 93726

In [1] a group-theoretical technique was employed to prove the following:

Theorem 1. Let

$$m = 2^e p_1^{e_1} \cdots p_k^{e_k}.$$

The congruence $x^2 \equiv 1 \pmod m$ has 2^k solutions if $e = 0, 1$, 2^{k+1} solutions if $e \geq 2$.

We extend this method to study the structure of the reduced residue system. Since the reduced residue system mod m is isomorphic to the automorphism group of cyclic group of order n, we need several lemmas on automorphism groups. Because of the existence of primitive root mod p^n, we have

Lemma 1. The automorphism group $A(C_{p^n})$ of the cyclic group of order p^n is cyclic, and its order is

$$\phi(p^n) = p^n - p^{n-1}.$$

Lemma 2. $A(C_{2^n})$ is cyclic if $n = 1, 2$. If $n > 2$,

$$A(C_{2^n}) = C_{2^{n-2}} \times C_2.$$

Proof. The first statement is obvious. For $n > 2$, the automorphism σ of C_{2^n} defined by $\sigma(a) = a^5$ has order 2^{n-2}; in fact if $n = 3$,

$$\sigma(a) = a^5, \qquad \sigma^2(a) = a,$$

so $|\sigma| = 2$. By induction on n,

$$\sigma^{2^{n-2}}(a) = a^{5^{2^{n-2}}} = a^{(5^{2^{n-3}})^2} = a^{(1+2^{n-1}+k2^n)^2} = a^{1+2^n} = a \quad \text{on} \quad C_{2^n},$$

i.e., $\sigma^{2^{n-2}}$ = the identity automorphism on C_{2^n} but $\sigma^{2^{n-3}}$ is not, so $|\sigma| = 2^{n-2}$.

Next we show that every automorphism α on C_{2^n} is a product of a power of σ and an automorphism τ of order 2. Let α be defined by $\alpha(a) = a^t$, where t is odd, we have

$$\alpha(a) = a^{(-1)^{\frac{t-1}{2}} 5^i},$$

i.e., $\alpha(a) = \sigma^i \tau(a)$, where

$$\tau(a) = a^{(-1)^{\frac{t-1}{2}}}.$$

Theorem 2. Let

$$m = 2^e p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n},$$

where $e \geq 0$, $e_i \geq 1$. The reduced residue system mod m is generated by the powers of $n + k$ elements, with

$$k = \begin{cases} 0 & \text{if } e = 0 \text{ or } 1 \\ 1 & \text{if } e = 2 \\ 2 & \text{if } e > 2. \end{cases}$$

Proof.

$$C_m = C_{2^e} \times C_{p_1 e_1} \times \cdots \times C_{p_n e_n} A(C_m) = A(C_{2^e}) \times A(C_{p_1 e_1}) \times \cdots \times A(C_{p_n e_n})$$

$$A(C_{2^e}) = \begin{cases} (1) & \text{if } e = 0 \text{ or } 1 \\ C_2 & \text{if } e = 2 \\ C_{2^{e-2}} \times C_2 & \text{if } e \geq 3. \end{cases}$$

REFERENCE

1. H. S. Sun, "A Group-Theoretical Proof of a Theorem in Elementary Number Theory," *The Fibonacci Quarterly*, Vol. 11, No. 2 (April 1973), pp. 161–162.

[Continued from P. 328.]

****

TABLE 3

Jacobi Symbols: $b = 5$

a	(a/b)	(b/a)	$(a/-b)$	$(-b/a)$
−7	−1	−1	1	−1
−5	0	0	0	0
−3	−1	−1	1	−1
−1	1	1	−1	−1
1	1	1	1	1
3	−1	−1	−1	1
5	0	0	0	0
7	−1	−1	−1	1

TABLE 4

Jacobi Symbols: $b = 7$

a	(a/b)	(b/a)	$(a/-b)$	$(-b/a)$
−7	0	0	0	0
−5	1	−1	−1	1
−3	1	1	−1	1
−1	−1	1	1	−1
1	1	1	1	1
3	−1	1	−1	−1
5	−1	−1	−1	−1
7	0	0	0	0

Then

$$\left(\frac{(a/-1)}{(b/-1)} \right) = 1$$

if and only if a is positive and/or b is positive; and

[Continued on P. 333.]